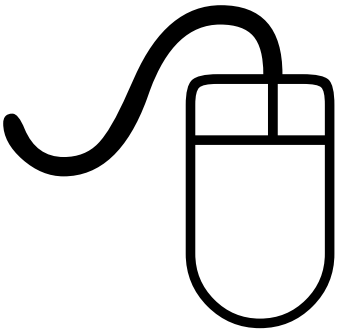
Whitley Academy
an RSA academy

E-SAFETY ADVICE



Guidance for Parents and Carers

RSA Opening Minds
An RSA Opening Minds Training School

INTRODUCTION

"A useful way for us all to think about this is to look at how we protect children in places of benefit and risk in the real (offline) world: public swimming pools. Here there are safety signs and information; shallow as well as deep ends; swimming aids and lifeguards; doors, locks and alarms. However children will sometimes take risks and jump into waters too deep for them or want to climb walls and get through locked doors – therefore we also teach them how to swim. We must adopt the same combination of approaches in order to enable out children and young people to navigate these exciting digital waters while supporting and empowering them to do so safety." Dr Tanya Byron, The Byron Review.

The internet is a wonderful and diverse place, filled with incredible information resources. Yet for many parents and careers, who often have less knowledge and experience of the internet, it can be a place of concern. We worry about what or whom our children may encounter while online, and how we protect them with our own limited knowledge. While we use it for booking holidays and answering emails, your children are setting up social networking pages, instant messaging with webcams, blogging, researching school projects, listening to music, playing online games and emailing friends.

Most children use the internet safely and responsibly and we shouldn't therefore lose sight of the positive aspects. As parents, we need to balance our concerns about their safety online with empowering them to explore and make the most of this wonderfully rich resource, safe in the knowledge that they can talk to us about anything they may run into.

In clear simple language, this booklet explains to parents what children already know or need to know about the online environment as well as providing advice about how you can protect your family, allowing them to use the internet safely and securely while having as much fun as possible.

This guide includes information and guidance about:

- ✓ Top Tip for Parents
- ✓ Social Networking and Instant Messenger
- ✓ Online Gaming and Games Consoles
- ✓ Grooming
- ✓ Cyber Bullying
- ✓ Computer and Online Security
- ✓ Identity Theft
- ✓ Mobile Phones
- ✓ Useful Websites
- ✓ Acceptable Internet Use at Home

TOP TIPS FOR PARENTS

1. Set up an account for each user on the PC at home and only give yourself administrator access. This will allow you to keep control of the settings and the installation of software. Each user account can be password protected. You can do this in the 'Control Panel'.

2. Add a screen saver protected by a password to your account so that if you leave the PC for 5 minutes you will have to enter your password. You can do this in the 'Control Panel'.

3. Encourage your family to use technology in a public part of the house, and not in the bedroom, where it's easier to monitor what your children are doing. This applies not just to PCs but also to laptops and games consoles. If a predator sees a living room/kitchen in the background on the webcam rather than a child's bedroom, they will be less likely to embark on attempting to groom your child.

4. Remember that many games consoles come with family settings. For example if you want to disable or limit 'Xbox Live' on the Xbox 360 you can do so by going to 'Settings, Parental controls'. There is also the option to add a mask to voices so that a youngster's voice sounds like that of an adult or even a robot. See the 'Online Gaming and Games Consoles' section for further information.

5. Encourage your child not to open emails from unfamiliar email addresses and to avoid opening suspicious attachments. As far as possible you should encourage your child to use the school's email system and Learning Platform as this provides a safer environment.

6. Set your favourite search engine to do 'safe searches'. This will make sure that a search returns content suitable for all ages. For example, to set Google to do safe searches click on search settings on the homepage and then ensure that moderate or strict filtering is enabled.

7. Tell children not to give out their personal details whilst online. If they want to subscribe to any online services or websites make up a family email address and ensure filtering is enabled.

8. The internet is a great resource for homework, but remember to use more than one site in research to get broad, balanced information and always reference your research sources.

9. Involve your children in writing your own family code of 'Acceptable Computer & Internet Use'. Remember that what's acceptable for a teenager isn't necessarily ok for a primary school-aged child, so get their input. See the 'Activities for use at home' section.

10. Surf together and engage in their world. Go online with your child and become part of their online life-add them as friend on a social networking site (once they're old enough), text them and discover what their game consoles can do. Keep up… today's technology is tomorrow's antique!

SOCIAL NETWORKING AND INSTANT MESSENGER

Social networking sites are amongst the fastest growing phenomena on the internet. Among the most popular social networking sites are Facebook, Bebo, MySpace and Twitter. All of them provide brilliant ways to stay in touch with friends and share photographs, comments or even play online applications. If used carelessly, however, they can expose you and your children to identity theft and online predators.

Instant messaging (IM) is a technology which enables you to send and receive messages almost instantaneously across an internet connection. IM is much faster than email and is rapidly replacing the telephone as the primary method of a quick or instant communication. Examples of IM are MSN, Windows Live, Yahoo! And even Facebook has its own IM service

Simple Social Networking and Instant Messenger Rules

Pay attention to age restrictions – for example Facebook and Bebo are only for people aged 13 year and older.

Social networking sites, such as Facebook and Bebo, have a range of privacy settings. These are often set up by default to 'expose' your details to anyone. When 'open' anyone could find you through a search of the networking site or even through a search engine, such as Google. So it is important to change your settings to 'Friends only' so that your details and profile content can only be seen by your invited and accepted friends and don't forget to remove yourself from search engine results.

Have a neutral picture of yourself as your profile image. Don't post embarrassing material!

You do not need to accept friendship requests. Reject or ignore unless you know the person or want to accept them. Be prepared that you may receive friendship requests or suggestions from people you do not know. It is not a competition to have as many friends as possible!

You can delete unwanted 'friends' from your Social Networking sites and IM lists. On IM don't forget to 'Block' them as well so they can't request your friendship again.

Exercise caution! For example in Facebook if you write on a friend's wall all their friends can see your comment – even if they are not your friend.

If you or a friend are 'tagged' in an online photo album the whole photo album may be visible to their friends, your friends and anyone else tagged in the same album.

You do not have to be friends with someone to be tagged in their photo album. If you are tagged in a photo you can remove the tag, but not the photo.

Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a website. If you are over 18 the web site will only look into issues that contravene their terms and conditions.

For more information visit:

www.thinkuknow.co.uk/parents/faq/socialnetworking.as
px www.thinkuknow.co.uk/parents/faq/chat.aspx

PRIVACY SETTINGS ON FACEBOOK

Facebook Privacy information can be found here:

http://www.facebook.com/home.php?#!/privacy/explanation.php

The safest way for your Facebook profile to be set-up is for it to be as private as possible i.e. only allowing your FRIENDS to have access to your information and pictures. It is therefore advisable that you only have REAL friends as contacts on Facebook and other Social Networking sites.

Please see the image below of the ideal set-up from a Facebook profile. You can find this by following these steps:
Click on Account in the top right hand corner of your Facebook page.
Choose the Privacy Settings option.
You will then see the page below and you can edit the settings to ensure the Friends only have access to your profile and its information.

ONLINE GAMING AND GAMES CONSOLES

More than ever games are heading online. Everything from Scrabble to World of Warcraft can be played online and against other human opponents rather than computer controlled opponents, which can be a lot more fun. Players can usually communicate with one another: perhaps using onscreen messaging which is typed during the gameplay or some games allow voice communication so that players can swap their thoughts freely whilst competing just like a telephone conversation.

Today's games consoles can be a great way to bring the family together for endless hours of fun. Whether it's bowling on the Nintendo Wii or Premier Manager on the Sony PlayStation, families can be involved in activity to develop communication and relationships.

The very best gaming however is safe gaming – which means games should be played responsibly. The ideal way to ensure that your children and teenagers are playing the right games, and playing sensibly, is to take an active interest in what they are playing.

Whether you children play games on a PC, Xbox 360, Nintendo Wii or Sony PlayStation, their gaming choices can be safely steered by you.

Play Safe Gaming Tips:

ENGAGE – find out what your children are playing and take an interest. Better still, join in the fun and play along yourself!

LIGHTEN UP – Games should be played in well-lit rooms. Darkened rooms, where games are played on old TV sets, have been known to trigger epilepsy issues.

TAKE BREAKS – Some games can be especially intense, so regular breaks are vital for healthy gameplay. Encourage your children to take regular breaks at least every 45 minutes.

BE AWARE – Explain to your children how the online world differs from home or the school playground. Online your children will meet total strangers – some who may not be who they say they are. Often the chat will be uncensored, so they should be cautious about what they say and be careful not to give out private details such as their name, address, email address, passwords, telephone numbers or the name of their school.

TAKE CONTROL – Take advantage of Parental Control setting available on your PC or games console. You can also decide which games are played by age rating and the PEGI descriptors or whether interaction which other games players is permitted at all. See page 6 for more information regarding this.

For more information about online gaming visit:
www.askaboutgames.com

GAMES CONSOLES

On the PlayStation 3 ® guardians can set security levels to restrict access to games depending on age ratings. DVD and Blu-ray movies can also be blocked completely.

To set security levels:

1. To set game level, from the Main menu scroll across using the ⬅ ➡ to settings and then down to **Security Settings**. Press ⊗ to select.
2. Scroll down to **Parental Controls** and press ⊗**.**
3. Enter your PIN Number then press ⊗ (the default PIN Number if you have not previously changed is 0000).
4. Select required **Security Level** by scrolling from **Off** to **Levels 1-11**. Press ⊗ to confirm.
5. The following settings provide a guide corresponding with **PEGI** ratings:
   2- PEGI 3+ **3 –** PEGI 7+ 5- **5-** PEGI 12+ **7 -** PEGI 16+ **9-** PEGI 18+
6. The PIN can be changed from the **Security Settings** menu.

The XBOX 306® allows you to restrict access to games depending on a game's age classification. You can also add a timer, restricting just how long each day or weeks your children can play.

1. From the Main menu scroll across to the **System Tab** on the right using ⬅ ➡
2. Scroll down to the second option on this tab. **Family Settings** and press the **A** button to select.
3. Scroll on **Console Controls** and press **A**.
4. Enter you 4 digit pass code (if you haven't previously set a pass code you will need to set one on the **Control Consoles** menu by selecting **Set Pass Code**).
5. Scroll to **Games Ratings** and press **A**
6. Now scroll to the age rating you wish to apply and press **A**. Users will be able to play games up to but not over this rating.

To limit games played by time:

1. Scroll to **Family Timer**, and on the **Console Controls** menu press A.
2. Scroll up and down to choose daily or weekly limits and press **A**.
3. Then scroll to the time bar ◀ **45 minutes**▶ and ⬅ ➡ to set usage time in minutes.
4. Scroll down to **Continue** and press **A**. Exit and save the settings by scrolling down to **Done** and press **A**. When you are asked if you wish to save the settings, scroll to **Yes**, save changes and press **A**.

The Wii™ allows you to restrict access to game's on age classifications. But this console also allows parents the chance to limit online communication with others.

To restrict games played by classification:

1. Use the Wii remote to move the cursor over the Wii button in the bottom-left corner of the screen and press the **A** button.
2. Click on **Wii Settings**.
3. Press the blue arrow ▶ to reach the Wii System Settings 2 menu options.
4. Select **Parental Controls** and confirm.
5. Enter you 4-digit PIN in the white box (if you have not already set a PIN you will be prompted to do so now). Click **OK** and again to confirm.
6. Click on **Games Settings and PIN**.
7. Now adjust the highest Game Rating Allowed by clicking on this option. On the menu that appears next, use the blue arrows ▲▼ to scroll to the desired setting. Once you have made your selection, hit OK. Click Confirm and then, on the next screen, **Settings Complete**.

For more information about consoles visit: www.askaboutgames.com

GROOMING

Online grooming is:
'A course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes.' Sexual Offences Act, 2003.

Often, adults who want to engage children in sexual acts, to talk to them for sexual gratification will seek out young people who desire friendship. They will often use a number of grooming techniques including building trust with the child in more intimate forms of communication, including compromising a child with the use of images and webcams. Child sex abusers will often use blackmail and guilt as methods of securing a meeting with a child.

How would I know if my child was being groomed?
There is no way of knowing without speaking to your child but there are some behaviours to look out for:

- Excessive use of the computer
- Aggressive behaviour regarding internet usage.
- Secretive behaviour
- Change in use of sexual language.

If you are concerned, talk to your child and review the sites they have been regularly.

For more information visit: http://www.thinkuknow.co.uk/parents/faq/grooming.aspx

CYBER BULLYING

Technology gives our children more ways to connect, socialise and communicate that ever before. Unfortunately, some children and young people use email, Instant Messaging, and mobile phones photos and text messages to embarrass or bully other children. Children's digital messages can also be edited to change the meaning then forwarded to others to embarrass, intimidate or insult.

According to research carried out for the Anti-Bullying Alliance in the UK 22% of young people reported being the target of cyber bullying.

Make sure your children know they must guard even the most casual text message and watch their own written words. They should never retaliate, and they should always tell you if and when they are being cyber bullied.

Keep a copy of any bullying message received via a PC or laptop by using the 'Print Screen' key on your computer keyboard and copying the message into a word processing program (e.g. Word). Likewise do not delete text messages or voicemails which also contain evidence of bullying.

For more information visit: http://www.kidscape.org.uk/childrenteens/cyberbullying.shtml

COMPUTER AND ONLINE SECURITY

Computer viruses have been around for more than 25 years in various forms, but with the popularity of email and file exchange on the internet, the distribution of these threats has really taken off. These days many of the bad guys are international cybercriminals, motivated by financial gain through their illegal activities.

Spreading via email, Instant Messaging, infected social networking pages, and file-sharing sites, malicious software (malware) such as spyware, keystroke loggers and bots can cause you enormous trouble.

Spyware and keystroke loggers monitor your normal computer activity and then report your private data out via the Internet to the criminals. Bots (short for robots) are forms of software that can sneak into your computer and cause your PC to send out spam and phishing emails to others, without you even knowing. Bots can also be used to steal your personal information and wreak havoc on your credit including the unauthorised use of your credit cards and bank accounts.

Help keep your children and your computers safe by installing security software on your family's computers and making sure it's updated with the latest protection files. Tell your children not to turn off the virus scanner or firewall, even if they think it might speed up a game. It's just not a safe risk to take.

For more information visit: http://www.getsafeonline.org/

IDENTITY THEFT

Many children will not automatically know what 'private' information is and the importance of keeping this private both online and offline so you need to explain the concept that it's any data that individually identifies them and may allow a stranger access to personal or financial information. Private information includes real world data such as names, telephone numbers, addresses, sports club, school, even the name of a doctor.

Fraudsters can turn even a small clue into a full record on a child and parent. They, in turn, can trade and sell that private data to make money. It's surprisingly easy for people with such intentions to apply for credit in your child's name and get real world merchandise and money, while ruining the child's (or your) credit rating and good name.

If you do suspect you've been a victim of identity theft, you are entitled to request a report from any of the credit reporting services for a small administrative fee: Equifax, Experian, and Callcredit all follow this. Once you find evidence of identity theft, you will need to report it to your bank as soon as possible and you may also wish to discuss it with your local police force for advice and guidance. You can also put a 'freeze' on your credit record and those of your children to prevent strangers applying for credit in your names.

For more information visit: http://www.ico.gov.uk

MOBILE PHONES

You can now access the Internet on most mobile phones and whilst this access brings a world of incredible opportunities in terms of communication, interaction and entertainment, there are certain risks to children posed via the internet. These risks include accessing potentially harmful content, such as pornography, possible dangerous contact with strangers in chatrooms and commercial pressures like spam and intrusive advertising.

The UK Mobile Operators have recognised these risks and have taken steps to help you protect your child from potentially harmful content accessible via your mobile phone. There are also things you can do to block premium rate calls and texts.

This guide is written by children's internet charity, Childnet International, and gives you a checklist of important questions to ask your mobile operator when purchasing a mobile phone so that you can ensure you have the tools and support to help protect children and make sure they get the most out of using their mobile phones safely. www.childnet.com/downloads/mobilesQ.pdf

Questions to Ask	Background
Safety Advice • Ask for information and advice about the phone and the services that are available on it, so that you can ensure your children know how to sue it safely.	Your mobile operator is committed to providing you with information and advice on safe use of their service. Be sure to check that they are keeping you informed.
Internet Access • Does this phone have internet access? • Is there a filter to help block Internet content that is particularly harmful for children? • Is the filter switched on? If no, can you switch it on please?	All the UK Mobile Operators have to provide and internet filter on their phones to help block accessing material that is potentially harmful to children, such as pornography. However, with most operators you will need to ask your operator to activate the filter.
Registering the Phone • Is the phone registered for a child or for an adult user?	Being registered as a child user will mean that you cannot access material provided by your mobile operator or its partners that is rated as 18+, i.e. unsuitable for children.
Bluetooth-enabled Phones • Is this phone 'Bluetooth-enabled'? • How can I turn this off, or set it so the phone is not visible to others?	Bluetooth technology essentially enables your mobile phone to find and 'talk' to other Bluetooth-enabled mobile phones in the vicinity, or other enabled phones to 'talk' to your mobile. When activated on your child's mobile phone it means that they may received unexpected and unwanted messages from other Blue-tooth-enabled phone users nearby, and any personal information stored on your child's phone – for example their contact list – could be vulnerable. Switching off the Bluetooth option is safer as it makes the phone 'invisible' to other Bluetooth users.

Questions to Ask	Background
Premium Rate Call and Texts • Can you put a bar on all premium rate numbers? • If you can't bar these numbers, what services do you provide to protect the user here?	If you do find you have signed up for a reverse-billed premium rate service (where you pay to receive rather than send text messages, e.g. for ringtones or football score updates) and you do not want to continue this, then text STOP to the shortcode number you got the text from. This will end the service and your payments to it.
Chatrooms and Gaming • Can this phone access chatrooms or games where users can chat to each other? • Are these chatrooms or games moderated? • How are the chatrooms or games moderated?	Chatrooms or games (where you can chat to other users) what are provided by your mobile operator or its partners and which do not have an 18+ age-restriction must be moderated.
Nuisance/Malicious Calls • What number can I call to report receiving unwanted or abusive calls or messages?	Your mobile operator should have systems and procedures in place to help you deal with nuisance and malicious phone calls.
Reporting Abuse • Where do I report abuse of service? If for example I receive unwanted adult (18+) material on my phone while the filter is switched on, who should I report this to?	It is important to let your mobile operator know if their system is failing, both in order to protect yourself and others using the same service.
SPAM • What action is your Mobile Operator taking to prevent SPAM?	Your mobile operator will take action against SPAM, whether it is text, picture or email. Find out what action your mobile operator is taking and report any SPAM received on your phone to them.

MOBILE PHONE PROVIDER – ADVICE FOR PARENTS

http://explore.ee.co.uk/digital-living/online-security

http://protectourchildren.o2.co.uk/

http://parents.vodafone.co./

USEFUL WEBSITES

Sites for Parents

www.ceop.police.uk/reportabuse/

If you are concerned about something that may have happened while online, you can take control. If you are in immediate danger or want urgent help call 999 or contact your local police. Otherwise there are a number of ways to receive help and advice as well as the option to report any instance of sexual contact or harmful material to the Child Exploitation and Online Protection Centre. You are doing the right thing and by taking this action you may not only help yourself but also help make other people safer as well.

www.thinkuknow.co.uk/parents

Think U Know has a section with advice for parents, which is particularly useful for explaining terminology. Register to receive the 'Purely for Parents' monthly email.

www.childnet-int.org/kia/parents

Know IT All for Parents is a useful CD which parents can use with their children to make sure that they get the most out of the internet. There is some sample content available on the site. Clicking on home will take you to the Childnet International site.

www.dcsf.gov.uk/byronreview
Read Tanya Byron's independent review looking at the risks to children from exposure to potentially harmful or inappropriate material on the internet and in video games.

www.dcsf.gov.uk/ukccis/

The UK council for Child Internet Safety (UKCCIS) brings together organisations from industry, charities and the public sector to work with the Government to deliver the recommendations from Dr Tanya Byron's report.

www.getsafeonline.org

Get Safe Online provides information and advice on using the internet safely at home.

www.ofcom.org.uk

Ofcom have great advice for setting parental controls on mobile phones and digital television boxes.

www.bbc.co.uk/panorama

Watch Panorama's investigation into how paedophiles are using the internet, and social networking sites in particular, as a means of grooming unsuspecting youngsters for sex. 'One Click From Danger'.

Sites for Using with Children

www.bbc.o.uk/onlinesafety/

BBC Online Safety help you use the internet in a safe way. It links to sites that are kept up to date with useful information, along with explanations and helpful hints for you and your family to get the most out of the internet.

www.chatdanger.com

Chat Danger is appropriate for 7 – 14 year olds and covers how to be safe when using interactive services online.

www.kidsmart.org.uk

Kidsmart had advice for children under/over 11 as well as games. The SMART rules are useful to help young people remember how to stay safe.

www.internetsafetyzone.co.uk

The **Internet Safety Zone** has sections for parent and children over and under the age of 13. The content and presentation of the site for years is good.

Safe searching – information, images and videos

These are sites which are 'safe' to use when searching.

www.google.co.uk/intl/en/landing/familysafety

Google SafeSearch when you're searching on Google, you may prefer to keep adult content out of your search results. SafeSearch screens sites that contain sexually explicit content and removes them from your search results. While no filter is 100% accurate, SafeSearch helps you avoid content you may prefer not to see or would rather your children did not stumble across. You can modify your computer's SafeSearch settings by clicking on the Preferences link to the right of the Google search box.

www.pics4learning.com

Photographs on a safe site from the US.

www.arkive.org

Images and videos of life on Earth

www.dorlingkindersly-uk.co.uk/static/cs/uk/11/clipart/home.html

Clip art from Dorling Kindersley

http://office.microsoft.com/en-gb/images/?CTT=97

Microsoft clip art and other images